Synaptics Security Advisory

Synaptics Fingerprint Driver: Co-Installer Privilege Escalation through DLL Search Order Attack

CVE: CVE-2025-11772

CVSS 3.1 Score: 6.6(Medium) AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Drivers

All fingerprint driver packages which include CheckFpDatabase.exe are affected.

Impact

A carefully crafted DLL, copied to a specific folder, allows a local user to execute arbitrary code with elevated privileges.

Background

The CheckFPDatabase.exe utility is run with elevated privileges by the co-installer, during setup of the Synaptics Fingerprint Driver.

CheckFPDatabase.exe is launched from a folder which is writable by low-privileged users. It uses functions exported by system DLLs and the default search path to locate those DLLs.

A carefully crafted DLL, with the same name as a required system DLL, allows arbitrary code execution.

Technical Details

An attacker creates the C:\ProgramData\Synaptics folder and copies a malicious DLL with the same name as a system DLL.

Then, during installation of the Synaptics Fingerprint Driver, the CheckFPDatabase.exe application is copied to the same folder, and run by the co-installer with elevated privileges.

When the CheckFPDatabase.exe application is started, it loads DLLs required for execution. If one of these DLLs is hijacked by placing a malicious copy into the same folder as CheckFPDatabase.exe, the malicious DLL is loaded instead of the required system DLL.

Acknowledgements

Synaptics would like to thank Finlay Richardson (Reversec) for reporting this issue.

Vulnerable/fixed version information

Vulnerable Driver Family	Fixed Version (and later)	Driver Date
5.5.xxxx.1066	5.5.3537.1066	2025-11-05
5.5.xxxx.1052	5.5.4022.1052	2025-11-06

This table is applicable to all known vulnerable PCs. Drivers where the xxxx values are lower than the corresponding sub-minor version number in the fixed version should be considered vulnerable. For any other drivers that contain CheckFPDatabase.exe but are not in one of these version number families, please contact your PC manufacturer.